WHAT IS CLAIMED IS:

1. A time stamp certifying the existence of a digital document at a time, the time stamp comprising:

an identification of an issuing clock certified through a chain of at least one signed certificates to be synchronized with an accepted standard source of time, wherein each of the signed certificates certifies that two clocks are synchronized;

an identification of the time, wherein the identification of the time is provided by the issuing clock;

a document identifier based upon which the identity of the digital document can be verified; and

a cryptographic signature of a set of data comprising:

the identification of the issuing clock,

the identification of the time, and

the document identifier.

2. The time stamp of Claim 1, further comprising at least one the signed certificates.

3. The time stamp of Claim 1, further comprising the signed certificates.

4. The time stamp of Claim 1, wherein the document identifier is the document.

5. The time stamp of Claim 1, wherein at least one of the signed certificates is cryptographically signed.

6. The time stamp of Claim 1, further comprising a link through which the chain of certificates can be accessed.

7. The time stamp of Claim 6, wherein the link comprises an identification of a certifying clock.

8. The time stamp of Claim 6, wherein the link further comprises an identification of the time.

9. The time stamp of Claim 1, wherein the chain is of at least two certificates.

10. A method of creating an authenticatable time stamp certifying the existence of a digital document at a time, the method comprising:

providing an identification of a trusted source of time certified through a chain of at least one signed certificates to be synchronized with an accepted standard source of time, wherein each of the signed certificates certifies that two clocks are synchronized;

providing an identification of the time, wherein the identification of the time is provided by the trusted source of time;

providing a document identifier based upon which the identity of the digital document can be verified; and

generating a cryptographic signature by cryptographically signing a set of data comprising:

the identification of the trusted source of time,

the identification of the time, and

the document identifier.

11. The method of Claim 10, further comprising providing at least one the signed certificates.

12. The method of Claim 10, further comprising providing the signed certificates.

13. The method of Claim 10, wherein the document identifier is the document.

14. The method of Claim 10, wherein at least one of the signed certificates is cryptographically signed.

15. The method of Claim 10, further comprising concatenating the identification of the trusted source of time, the identification of the time, and the document identifier.

16. The method of Claim 13, further comprising additionally concatenating at least one of the signed certificates.

17. The method of Claim 10, further comprising providing a link through which the chain of certificates can be accessed.

18. The method of Claim 17, wherein the link comprises an identification of a certifying clock.

19. The method of Claim 18, wherein the link further comprises an identification of the time.

20. The method of Claim 10, wherein the chain is of at least two certificates.

21. A trusted clock configured to provide time, the trusted clock certified through a chain of at least one cryptographically signed certificates to be synchronized with an accepted standard, wherein each of the signed certificates certifies that two clocks have been determined to be synchronized.

22. The trusted clock of Claim 21, wherein each of the signed certificates identifies a time at which the two clocks have been determined to be synchronized.

23. The trusted clock of Claim 21, wherein each of the signed certificates identifies the two clocks.

24. The trusted clock of Claim 21, wherein the chain is of at least two certificates.

25. A certificate certifying that two clocks are synchronized, the certificate comprising:

an identification of a first clock;

an identification of a second clock;

an identification of a time at which the first clock and the second clock have been determined to be synchronized; and

a first cryptographic signature of a first set of data comprising:

the identification of the first clock,

the identification of the second clock, and

the identification of the time.

26. The certificate of Claim 25, further comprising a measured temporal offset between the first clock and the second clock, wherein the first set of data further comprises the measured temporal offset.

27. The certificate of Claim 25, further comprising an expiration time, wherein the first set of data further comprises the expiration time.

28. The certificate of Claim 25, further comprising a second cryptographic signature created by either the first clock or the second clock, wherein the first set of data further comprises the second cryptographic signature.

29. The certificate of Claim 28, wherein the first cryptographic signature is created by the first clock and the second cryptographic signature is created by the second clock.